

La AEPD publica ‘El estatuto del delegado de protección de datos’, con orientaciones sobre independencia, garantías organizativas y conflictos de intereses

El documento reúne los criterios de la Agencia sobre designación, posición, rendición de cuentas, garantías frente al cese y conflictos de intereses de las personas delegadas de protección de datos (DPD) en el sector público y privado

La Agencia Española de Protección de Datos (AEPD) ha publicadoEl estatuto del delegado de protección de datos. Orientaciones sobre el marco de actuación, independencia, garantías organizativas y conflictos de intereses, que reúne en un único texto los criterios de la Agencia sobre la posición de las personas delegadas de protección de datos (DPD) en las organizaciones. El documento recoge cómo deben designarse, qué garantías de independencia les corresponden, cómo rinden cuentas ante la alta dirección, qué protección tienen frente al cese y las represalias, qué funciones pueden generar conflictos de intereses y a qué vías pueden acudir cuando esas garantías no se respetan.

El DPD es la figura central del modelo de responsabilidad proactiva del Reglamento General de Protección de Datos (RGPD) y de la Ley Orgánica 3/2018 (LOPDGDD). Para la Agencia, los DPD son los mejores aliados del cumplimiento normativo. Por ello, el Plan Estratégico 2025-2030 les atribuye un papel central y se compromete a reforzar su independencia funcional y a formular propuestas para clarificar su estatuto jurídico. El documento responde también a la acción coordinada del Comité Europeo de Protección de Datos sobre los DPD, en la que participó la AEPD y cuyo informe señaló, entre otros aspectos, conflictos de intereses, falta de independencia, dependencia presupuestaria y dificultades de acceso a la alta dirección.

Qué establece el documento

El texto, que no tiene carácter normativo ni crea obligaciones nuevas, interpreta las garantías recogidas en los artículos 37 a 39 del RGPD y 34 a 37 de la LOPDGDD, a la luz de las sentencias del TJUE (Leistritz, X-FAB Dresden y KISA) y de la sentencia de la Audiencia Nacional de 18 de marzo de 2026, para ofrecer a los DPD y a las organizaciones un marco de certeza y seguridad jurídica. Sus principales contenidos son los siguientes:

- **Designación.** Debe ser formal, documentada y transparente, aprobada al más alto nivel y comunicada a la autoridad de control, a la plantilla y a las personas interesadas. Se recomienda formalizarla mediante una carta de misión o la correspondiente regulación contractual, evaluar los posibles conflictos de intereses antes del nombramiento y garantizar la continuidad de la función.
- **Independencia.** Se desarrolla en cuatro dimensiones: funcional (el DPD no recibe instrucciones sobre el contenido de su asesoramiento ni de su supervisión), jerárquica (rinde cuentas directamente al más alto nivel), económica (recursos suficientes y sin retribuciones variables que puedan condicionar su objetividad) y organizativa (acceso a los datos y a los sistemas de tratamiento, y consulta temprana desde el diseño de los proyectos).
- **Rendición de cuentas.** Los mecanismos de información a la dirección deben ser proporcionales al tamaño y al riesgo de cada organización. El RGPD no impone un modelo de informe ni una memoria anual. Lo relevante es poder acreditar esa comunicación. Si la organización se aparta del criterio del DPD, es recomendable dejar constancia de las razones.
- **Garantías frente al cese y las represalias.** La protección del artículo 38.3 del RGPD no equivale a una inamovilidad absoluta, pero alcanza a cualquier decisión desfavorable que afecte a su independencia en el ejercicio de la función; la LOPDGDD la refuerza para el DPD integrado en la organización, que no puede ser removido ni sancionado por desempeñar sus funciones, salvo que incurra en dolo o negligencia grave en su ejercicio. Las decisiones que afecten a su permanencia, funciones, recursos o posición deben examinarse por sus efectos materiales. La Agencia recomienda recabar antes su parecer, evaluar su impacto y

documentar las razones.

- **Conflictos de intereses.** El DPD asesora y supervisa, pero no decide sobre los fines y los medios de los tratamientos. El documento analiza, caso por caso y sin incompatibilidades automáticas, los puestos que pueden generar conflicto (alta dirección con funciones operativas, responsable de seguridad de la información, responsable del canal del informante, responsables de datos o de inteligencia artificial con poder de decisión), los potencialmente compatibles si no implican decidir sobre fines y medios (asesoría jurídica, cumplimiento, auditoría interna, transparencia) y situaciones de riesgo: representación legal de la organización, DPD externo que actúa a la vez como encargado, acumulación excesiva de clientes o funciones e insuficiencia de recursos.
- **Vías de amparo.** Ante presiones o injerencias, el DPD puede acudir directamente a la alta dirección y al canal interno de información, consultar o poner los hechos en conocimiento de la autoridad de control de protección de datos y, en su caso, acudir a los tribunales.

La idea que recorre el documento es que la independencia del DPD no es un privilegio personal, sino una garantía institucional que la organización debe hacer efectiva. Designar un DPD no traslada a esta figura la responsabilidad del cumplimiento, que sigue siendo del responsable o del encargado; lo que exige es dotarle de la posición, los medios y la autonomía necesarios para asesorar con criterio y supervisar con objetividad.

Un documento elaborado con el sector

El marco se ha elaborado mediante un proceso participativo y colaborativo. El texto se compartió con las autoridades autonómicas de protección de datos, con amplia y directa experiencia en el sector y en el marco de una colaboración intensa en diversas áreas. Asimismo, el borrador se sometió a dos rondas de consulta y diálogo con las asociaciones profesionales de la privacidad —el Club del Delegado de Protección de Datos de la Asociación Española para la Calidad (AEC), la Asociación Profesional Española de Privacidad e Inteligencia Artificial (APEP·IA), ENATIC e ISMS Forum— y con delegados y delegadas del sector público. Todas las aportaciones recibidas permitieron enriquecer el texto que ahora se publica. Este método responde al séptimo eje del Plan Estratégico de la Agencia, que prevé el diálogo previo con los sectores afectados antes de publicar guías y criterios.

Se han tenido en cuenta los precedentes españoles —entre ellos, el modelo de instrucción interna del Consejo de Transparencia y Protección de Datos de Andalucía y los informes y resoluciones de la propia Agencia— y las referencias del Comité Europeo de Protección de Datos, del Supervisor Europeo de Protección de Datos y de otras autoridades de control europeas.

Un documento abierto y próximas acciones

Este marco se concibe como un documento abierto. El primer complemento previsto es la concreción de buenas prácticas para la solución de conflictos de intereses en supuestos concretos, en colaboración con las asociaciones profesionales. La Agencia abordará también el análisis de la relación entre las funciones de protección de datos y las responsabilidades vinculadas a la inteligencia artificial, para delimitar sus ámbitos de actuación, prevenir conflictos de intereses y preservar la independencia de los DPD.

Esta publicación se suma a actuaciones como el proceso de diálogo con los DPD de la Administración General del Estado, que dio lugar en julio a unas recomendaciones para fortalecer el cumplimiento en el sector público y los encuentros periódicos con personas delegadas. La Agencia invita a los DPD, a las organizaciones y a las asociaciones profesionales a trasladarle sus observaciones sobre la aplicación práctica del documento.

Fuente: *AEPD*